TITLE:	PHYSICAL SECURITY		
POLICY #:	P-CCSP-010	**EFFECTIVE DATE:**	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	**SUPERCEDES:**	FIRST RELEASE

State of Colorado
Cyber Security Policies

Physical Security

Overview

This policy document is part of the State of Colorado Cyber Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). All Agencies within the scope of this Policy must support and comply with the Requirements section of this document. Additional best-practice guidance is outlined in the Guidelines Section which has been designed to help an Agency achieve the objective of this Policy.

For the purposes of this document, an “Agency” includes organizations as defined in C.R.S. 24-37.5-102(5).

Authority

C.R.S. 24-37.5-401(1), C.R.S. 24-37.5-403(2)(b)-(c), C.R.S. 24-37.5-404(2)(b).

Scope

This policy document applies to every State agency ("Agency") as defined in C.R.S. 24-37.5-102(5). "State agency" means every state office, whether legislative, executive, or judicial, and all of its respective officers, departments, divisions, commissions, boards, bureaus, and institutions. "State agency" does not include State-supported institutions of higher education, the department of higher education, the Colorado commission on higher education, or other instrumentality thereof.

Policy

Agencies shall limit physical access to the system, network, and data to only those authorized personnel who require access to perform assigned duties. Where systems are deployed in areas where controls may not completely restrict access to only authorized personnel, a compensating control must be deployed to identify unauthorized access to systems, networks, and data.

Definitions

For the purposes of this document, refer to C.R.S. 24-37.5-102, C.R.S 24-37.5-402 and the Colorado Cyber Security Program Policy Glossary for any terms not specifically defined herein.

Roles and Responsibilities

Executive Director – is responsible for ensuring that adequate funding is allocated to support the required physical controls identified in this policy and delegating of the role of Physical Security Personnel in lieu of having dedicated personnel on staff

Physical Security Staff or Personnel with Delegated Responsibility – are responsible for keeping all external doors locked at all times with exception of reception area door; responsible for activating all alarms (if applicable) and locking doors and windows when facility is unattended; and for revoking physical access and physical access tokens of terminated employees.

Agency Chief Information Officer (CIO) – is responsible for ensuring the physical locations used to house IT systems uphold the standards in this document and for ensuring IT Department Personnel are fully trained in physical security practices.

Agency Information Security Officer (ISO) – responsible for evaluating physical security controls for adhering to this policy in Agency Risk Assessment activities and making remediation recommendations that uphold this policy.

Agency IT Staff – is responsible for accompanying all visitors, vendors, and other unauthorized personnel while accessing computer room, datacenter or wiring closets and ensuring physical access to infrastructure components is controlled by monitoring access to sensitive IT systems.

Users – are responsible for not leaving user workstations unattended when logged into sensitive systems or accessing sensitive data and are responsible for positioning monitors and system terminals to limit inadvertent viewing by visitors or unauthorized system users.

Requirements

All departments are to develop Physical Security Plans that support the guidelines of this policy and are to document a Plan of Action and Milestones for modifying facilities that do not meet these standards.

All Agencies are required to define areas of their facilities that meet the following definition of a Sensitive Area:

> Sensitive Areas are areas within a facility that contain systems that store, process or transmit data on behalf of the State. The boundaries of this area are the closest doorways that provide access to this area. Separate Sensitive Areas may be grouped together to form a single Sensitive Area if there is a common ingress/egress point and if all individuals that would require entry through that common point have "need-to-know" established for all concentric areas.

Access to Sensitive Areas shall be granted based on approved requests in accordance with the Access Control Policy P-CCSP-008.

The following protective measures must be implemented by each Agency:

Building Perimeter Security

- All external doors except for a door into a reception area must be locked at all times and must require keys, cipher codes, or proximity badges to enter.
- All visitors obtaining access to Sensitive Areas must register at the reception area and remain supervised when on the premises.
- Doors and windows must be locked and alarms activated (if applicable) when the facility is unattended.

Internal Security

- Access to all infrastructure computing/networking devices (i.e., routers, hubs, firewalls, servers, Private Branch Exchanges (PBX), etc.) must be restricted to Agency staff with a demonstrated need for recurring access. Separate physical control and access verification must be provided for facilities housing these devices.
- Access to other network infrastructure components, such as network cables, must be controlled to prevent unauthorized intrusion into the network. At a minimum, internal network connection points (ports) are not to be available in unmonitored or unrestricted publicly-accessible areas. Where appropriate, these areas are to be secured and marked as restricted.
- When employment is terminated, all physical access to State of Colorado facilities must be revoked immediately and all physical access tokens (i.e., IDs, keys, magnetic stripe cards, etc.) must be recovered.

Workstation Security

Access controls policies and procedures for network access are governed by Access Control Policy, P-CCSP-008 and System and Applications Operations Policy, P-CCSP-007. In addition procedures are to be developed to using the following guidelines.

- Position work station monitors to limit inadvertent viewing by unauthorized personnel. If not possible monitor filters are to be used.
- User workstations must not be left unattended when logged into sensitive systems or accessing sensitive data. Automatic log off or password-protected screen savers that activate within 15 minutes are to be deployed to enforce this requirement where feasible.
- All equipment that contains sensitive information is to be secured to deter theft. In the case of mobile computing devices, all sensitive data must be encrypted when removed from State facilities. If this is not possible, the system must not be left unattended.

Data Center Security

- All agency data centers, computer rooms and wiring closets must be categorized as a Sensitive Area.
- An IT department representative must accompany all visitors, vendors and State staff that do not have the appropriate access credentials while accessing a computer room, datacenter or wiring closets.

- A record of all access to data centers and wiring closets is to be maintained for a minimum of one year.
- System backups are secured in accordance with System and Applications Security Operations Policy, P-CCSP-007.
- Datacenters must have automatic fire protection systems installed.
- At a minimum, all systems within the datacenter must be supported by a power-conditioning Uninterruptible Power Supply (UPS) that provides adequate time to shut down systems per the system hardware or software vendor's recommendations.

Guidelines

This section describes best practices for meeting the objective of this policy.

Building Perimeter Security

- All external doors except for a door into a reception area are to be locked at all times and to require keys, cipher codes, or proximity badges to enter.
- All visitors obtaining access to areas of State facilities where sensitive data or equipment is stored must register at the reception area and remain supervised when on the premises. An IT department representative must accompany all visitors, vendors and State staff while accessing a computer room, datacenter or wiring closet.
- Doors and windows are to be locked and alarms activated (if applicable) when the facility is unattended.

Internal Security

- Support equipment such as fax machines are to be placed in secured areas to avoid inadvertent access, which could compromise information. The secure areas are to be positioned to monitor access to the sensitive systems. If physical monitoring is not possible, the department manager should consider placing a video monitoring device to meet monitoring requirements.
- Unique User Identification is required for entry to Sensitive Areas.

Data Center Security

- Perimeter walls of the Datacenter are to be floor-to-ceiling (sub-floor to ceiling slab) and properly sealed to ensure effectiveness of access controls, cleanliness and cooling.
- A CCTV or other monitoring system is to record all entry and exit in the Data Center.
- Card key access is required to gain entry into rooms storing sensitive systems and data. Key code entry is an alternative only if the key coded access is combined with video monitoring.
- The card key system is to record date, time and card holder name for all users entering the room and must enforce user privilege restrictions.
- The rooms and doors are to be constructed with sufficient strength to deter entry by an intruder and are to cause significant damage if an intruder attempts unauthorized access.
- Each critical device is to be served by dual power sources. In the event one power source fails the second power source continues operations for at least 15 minutes.

- Each room storing sensitive systems and data should be protected with a smoke detection and a class C fire suppression system in the datacenter or computer rooms. Fire suppression equipment is to be inspected annually to validate that it meets specifications and local ordinances.
- Fire alarms and a Type C Fire extinguisher are to be available in all State of Colorado computing facilities in case of an electrical fire.
- Local fire departments are to be informed of the existence of the datacenter and coordination of fire procedures.
- A UPS is to be used to power all server equipment.
- Generators are to be in place to provide continuous electrical power in the event of an extended utility outage. Generators must also provide power to the HVAC and life-safety systems that support the datacenter.
- Before the addition of any new equipment, the IT department is to assure that rack capacity, electrical capacity, cooling capacity and bandwidth capacity are available as part of the department's Risk Management Processes.
- All flows of air, gas, and water into the computing facility must have shutoff valves and provide positive drains.
- Multiple layers of protection are to be instituted to protect access to the Data Center. Access to the Data Center requires an additional key or separate badges issued by or on approval from the agencies Information Security Officer.
- Emergency lighting is to be maintained in both the computer room and other areas of State facilities where sensitive information is stored.

References

- ISO 17799-2005, "Code of Practice for Information Security Management", Section 9, Physical Security
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12 Chapter 15
- State of Colorado Access Control Policy, P-CCSP-008
- State of Colorado System and Applications Security Operations Policy, P-CCSP-007
- State of Colorado Cyber Security Planning Policy, P-CCSP-001